intuit Pay

Card Processing Guide

Merchant Operating Instructions

Contents

Welcome to Intuit Pay

Welcome to Intuit Pay! Intuit Pay lets you accept card payments wherever you go so that you never miss a sale. We provide you with an easy to use mobile app, sleek Chip & PIN card reader, and web terminal so that you can start taking payments right away. Now we ask that you read through this guide to understand how we can work together to keep all our payments safe and secure. And we are always here to help you with any questions or issues: www.intuitpay.co.uk/support.

Introducing Intuit

At Intuit, we are driven by a desire to solve the important problems small businesses face every day. Our software and services provide practical help to save business owners time in getting on top of their finances, accounts and payroll.

We provide financial management software and services to help small businesses get on top of their finances, save time on their accounting, and take payments on the spot wherever they go.

Our products are designed to revolutionise people's financial lives. We work on the principle that everything should be easy to use, and we back our solutions up with the highest levels of service and support.

Our customers define who we are. Since our inception, we've dedicated ourselves to knowing them, watching them and listening to them. We even visit them in their workplaces, all to understand how they use our products and how we can make their lives easier.

Intuit was born at our founder's kitchen table in 1983. Today, it has global revenues which top £3bn, approximately 8,000 employees and major offices in the United States, Canada, the UK, India and other locations.

About This Document

This *Merchant Operating Instructions*, together with the other documents listed in clause 1 of the *Terms of Service*, constitutes the Card Processing Agreement you are making with us (the “Agreement”).

For your own benefit and protection you should read this document and the terms of service carefully before accepting as they form part of your Agreement upon which we intend to rely. If you do not understand any point, please ask for further information. See page 31 for our contact details.

What Do These Merchant Operating Instructions Tell You?

These instructions provide you with:
→ an overview of the various ways in which we can support your business; and
→ information about our charges and other operational instructions.

Please Read This Document Carefully As It Contains Critical Information To Help You Avoid Fraud.

The instructions include critical information about the risks associated with cards as a method of payment. They also highlight some vital steps that you should follow to help raise your awareness and minimise your exposure to these risks.

Please follow the procedures detailed in these instructions carefully. They will enable you and your business to gain the maximum benefit from accepting card payments.

You should also keep a copy of these *Merchant Operating Instructions* somewhere convenient so that you and your employees can easily access them when required, but **where customers or any other parties cannot access them**. If you cannot find the information you need please contact us (see page 31 for our contact details).

Please Keep Us Informed If Your Business Changes

There are risks involved with card processing and we feel that it is our duty to ensure that you are aware of these risks. We will keep you informed of developments in the industry, including trends in fraudulent activity and advances in anti-fraud processes and technology. This will help you maintain your security at the highest level and reduce the potential risk to your business.

To ensure we can keep you informed and ensure you are receiving the services appropriate to your situation, please let us know if any of your business details change, such as:

- your contact details (including e-mail address or telephone number);
- your business address;
- the type of business being conducted by you;
- significant changes in the volume of business you are experiencing;
- you intend to change the way you conduct business, for example, starting to trade remotely or via the internet
- change in significant shareholding (usually defined as 25% or more); or
- you sell your business or change its legal entity.

In particular, if you change your business address, correspondence address, contact details or telephone number you need to inform us via email to: support@intuitpay.co,uk

For more information on this procedure or to advise us of any of the other types of changes listed above, please email us at: support@intuitpay.co.uk

Please Contact Us If You Have Any Questions Or Feedback

Our aim is to provide you with the highest possible level of service. As such, we welcome all your comments and feedback. Please feel free to get in touch if you have any questions or comments about these instructions, or any aspects of the card processing service we provide.

An Introduction To Card Processing

Card processing can provide numerous benefits to your business including:
→ improved cash flow;
→ improved decision making with easy access to your transaction history
→ provision of an alternative payment method;
→ accepting payments remotely

Card processing enables you to accept card payments from your customers in a number of environments and can be broadly split into two groups of transaction types:

- **Card Present (CP)** transactions, which means any transaction where the card and cardholder are physically present with you at the time of the transaction and where you can evidence the presence of the card tendered either by chip read or card swipe through an electronic terminal and includes the following types of transaction:
  - sale transactions for the sale of goods or services
- **Card Not Present (CNP)** transactions, which means any transaction where the card and cardholder are not physically present with you at the time of the transaction and includes the following types of transaction:
  - mail/telephone/fax transactions conducted by post, fax, telex, telephone or any other similar form of communication (see page 17)
  - internet transactions via computer networks including the internet

Your *Service Schedule* details which transaction types you are authorised to accept. You must have our written authority before you can process any other transaction types.

Risk Awareness

We want your business to accept cards effectively and without problems. However, it is vital that you are aware of, and understand, the risks associated with accepting cards.

One such risk is a chargeback, which is an unpaid card transaction that has been returned to us by the card issuer. We may debit the chargeback to your account, however, this section highlights some of the ways you can minimise the risk of chargebacks to your business.

There is no guarantee of payment for any transaction, even if you obtained authorisation. Authorisation checks that at the time of the transaction, the card is not reported lost or stolen and that the genuine cardholder has sufficient funds available. Authorisation cannot verify that the genuine cardholder is conducting the transaction.

Never spread the value of the sale over more than one card, or split the sale into smaller amounts.

Card Present (CP)

Chip And PIN Transactions

Chip and PIN is currently one of the most secure methods of card payment and should be used where the cardholder and merchant are together during the transaction. Non chip and pin transactions make your risk of liability for fraudulent transactions significantly higher.

Even if your point of sale equipment accepts chip and PIN transactions you must still seek online authorisation if you accept a chip and PIN card or a chip and signature card using the magnetic stripe and signature as verification (see ‘Authorisation’ on page 14).

Magnetic Stripe Transactions

Although chip and PIN has become the norm in the UK, you will still occasionally need to accept magnetic stripe transactions, for example when:

- → non-chip cards are presented – usually cards issued outside of the UK, such as in the United States of America, where magnetic stripe cards are still predominantly used
- → using the magnetic stripe as a result of problems with the chip – pay particular attention to these transactions as the chip could have deliberately been interfered with to avoid validations via the PIN.

In these cases, the transactions will be authorised online and you will need to carefully check that the customers' signature matches that on the card. Please follow the instructions on page 9 *(Checking Cards)*. A Copy of the electronically signed receipt will be stored in the online portal?

Card Not Present Transactions (CNP)

These situations are ideal for fraudsters because the card, signature and personal identification number (PIN) cannot be checked as you, the card, and the cardholder are **not** all present together. The majority of chargebacks result from transactions being undertaken fraudulently. If you proceed with a transaction that you are unsure of, you are doing so at your own risk. If the transaction has been completed, but the goods not despatched, you are still in a position to carry out a refund. Refer to page 16 for further information on CNP.

To Minimise CNP Risk

When accepting orders:

- → Be cautious of customers who give mobile phone numbers as their only form of contact.
- → Be wary of an order emanating from an e-mail account where the customer's name is not reflected in the e-mail account address.
- → Be suspicious with transactions that have an unusually high value or volume for your type of business or the sale is 'too easy'. In our experience these are the more likely ones to be fraudulent.
- → When performing a refund, always refund to the same card used for the original transaction.
- → Keep a database of chargeback history to help identify patterns of fraudulent transactions. If a sale seems too good to be true then it probably is. Do not be afraid to contact the cardholder to ask further questions or request additional identification. A genuine customer should be pleased you are security minded and trying to protect them from fraud.
- → Where possible, perform Address Verification Service (AVS) and Card Security Code (CSC) checks (see page 11). Refer to your terminal manual or terminal supplier for assistance on using this security feature. Remember that you are **not** allowed to store the CSC data.

When delivering goods:

- → Always send goods by recorded or special delivery or by a reputable security carrier. Insist on a signed (preferably by the cardholder) and dated delivery note. Tell the courier not to make the delivery if the premises appear to be vacant. Please note that proof of delivery alone is not sufficient evidence to defend a chargeback.
- → Do not release goods to third parties such as taxi drivers and messengers.
- → Be cautious of transactions where the billing address is different to the requested delivery address. Avoid delivering to addresses other than the cardholder's, such as hotels, internet cafes and 'care of' addresses.

- → Be wary of requests for next-day delivery, requests to alter the delivery address at short notice, or telephone calls on the day of delivery requesting a specific delivery time.
- → If a customer requests to collect the goods, perform the transaction at the time of collection through your point of sale equipment.

Please see page 26 for further information on how to help avoid CNP fraud.

You risk receiving a chargeback if the transaction is successfully disputed. We may debit the value of the transaction to your business.

Remember authorisation is not a guarantee of payment (see 'Authorisation' on page 14).

Data Security

Security of personal data is a growing concern. Criminals are always looking at ways of getting this type of information from different sources. A vulnerable point of compromise which fraudsters have identified is card financial data which has been collected during the acceptance of cards. The Payment Card Industry Data Security Standard (PCI DSS) is a global mandated standard which has been introduced by the Card Schemes to bring a greater level of security to this type of data.

As you are accepting card transactions, you need to be aware of the value of the data you collect when undertaking a card transaction and the need to secure it. If you were to suffer a security breach, there is a significant risk of financial and reputational loss to your business.

Merchants who accept CNP transactions are required to achieve and maintain PCI DSS compliance due to the higher risks of data breaches in a CNP environment.

For further details on PCI DSS, please go to page 24 or you can visit www.pcisecuritystandards.org. This site holds the latest version of the PCI DSS specifications and guidance on how to become compliant.

Processing Third Party Transactions

Processing transactions on behalf of another business can severely damage your financial well being. If you are either offered a lump sum for allowing unlimited access and usage of your card processing facility or a commission for each payment you process, be wary that it is very rare for the third party to deliver the service that was promised. Often these entities, whilst appearing to be genuine and providing plausible reasons for requiring assistance are fronts for organised criminal gangs engaged in timeshare or ticketing scams.

You must **never** accept transactions on this basis. These transactions are usually disputed or fraudulent, and could result in chargebacks and financial losses to your business. Should this be the case you will be fully liable for reimbursing the cardholders where non-provision of the goods or services has occurred.

Third party processing also breaches your Card Processing Agreement with us, and identification of such activity may result in immediate suspension and eventual termination of your card processing facility. This type of processing can also lead to criminal proceedings.

If a third party approaches you, or your staff, to process their transactions, say no and contact us straight away with as much detail as possible. If you feel your business may have already succumbed to such a deception, or has recently received an approach, then

please call us immediately for assistance with as much information as possible so that we can take appropriate action.

Copies Of Sales Vouchers

We may request information relating to specific transactions at any time. Please respond immediately to any such request as failure to do so may result in a chargeback.

Terminals

You are responsible for the terminal equipment and we strongly recommend that due consideration is given to the positioning and control of such equipment. You will be responsible for any losses resulting from interference by third parties not authorised to manipulate the equipment in any way other than in the normal course of the transaction, for example, entering a PIN.

Card Present Transactions

Card Present (CP) transactions are any transaction where the card and cardholder are physically present with you at the time of the transaction and where you can evidence the presence of the card tendered either by chip read or card swipe through an electronic terminal and includes the following types of transaction:
→ sale transactions for the sale of goods or services

Checking Cards

The type of card will determine which validation checks are needed.

Cardholder Verified By PIN

You should hand the card reader to the cardholder who will insert the card into the card reader.

The requirement to undertake physical and visual validation checks on the card will depend upon whether you actually handle the card at any time during the transaction. If you do handle the card, then you must follow the procedures detailed in ‘How to Perform Card Validation Checks’ on this page. There is however no need to obtain a customer signature on the terminal receipt

Cardholder Verified By Signature

There are certain circumstances when the identity of the cardholder cannot be verified by the use of a PIN. These include:
→ a card with no chip (for example a magnetic stripe card)
→ a chip card that does not use the PIN as its verification method.

In these circumstances the cardholder will not be prompted to enter a PIN. If a card is verified by signature, you must follow the procedures detailed in the section below.

How To Perform Card Validation Checks

There are many different designs of credit and debit cards. Please see the following section for some examples of card types. The validation checks listed below apply to the majority of cards issued by any bank or other financial institution. Failure to follow these checks may result in you being subject to a chargeback:

1. Chip
→ If there is a chip on the card, check if there has been any visible attempt to remove, replace or damage it.

2. Card Number
→ The cardholder account number always begins with a 5 for MasterCard and a 4 for Visa
→ for MasterCard and Visa, the first four digits of the account number are repeated above or below the beginning of the embossed card number – make sure they match the first four digits of the embossed number
→ the last four digits of the card number on the front of the card must match the number on the reverse on the signature strip, if present, and also the last four digits of the card number printed on the terminal receipt
→ for embossed cards, check the numbers. If the area around these is distorted, the original numbers may have been flattened and fake numbers added
→ the account number on the front of the card may be printed rather than embossed, and so feels smooth rather than raised.

3. Cardholder Title And Name
→ Check for obvious discrepancies between the cardholder and card, such as a woman using a card with the title ‘Mr’, or a teenager using a card with the title ‘Doctor’ or ‘Sir’
→ some cards include a photograph of the cardholder. You must check that the photograph matches the person presenting the card and that it has not been tampered with.

4. Expiry Dates/Valid From
→ The card should be carefully examined for the effective validity date. You must not accept cards presented before their ‘valid from’ date (where shown) or after their expiry date. The terminal will perform certain checks on the card, but we cannot be held liable if the terminal accepts a pre-valid or expired card.

5. Hologram
→ Check that it has not been tampered with. The hologram should be smooth to the touch, should not have a rough or scratched surface and the 3D image should move when tilted. Counterfeit cards often feature poor hologram reproductions
→ the hologram can be on the front or back of the card unless a Holomag tape (holographic magnetic stripe) is used in place of the traditional magnetic stripe
→ the most common designs are:
  → MasterCard - the world
  → Visa - a dove, which appears to fly
  → Visa Electron - not all cards contain a hologram. When present, the hologram will appear as a flying dove.

6. Signature Strip
→ Remember, if the card is verified by PIN, you do not need to check that the signature matches
→ the signature should be written clearly and be smooth to the touch. Be suspicious if the card is not signed, if the signature appears to have been erased, if the card appears to have been re-signed, or if the signature is written in block capitals or felt pen
→ check that the signature agrees with the name on the front of the card
→ check that the signature strip has not been tampered with or that the word ‘void’ is not visible
→ check that the signature on the card matches the one on the terminal receipt or voucher
if you are presented with an unsigned card, ask the cardholder for identification

7. Card Security Code (CSC)/Card Verification Value (CVV2)

→ A three or four-digit validation code. For MasterCard, Visa and Maestro cards the CSC is the last three digits printed on the reverse of the card after the last four digits of the cardholder account number, if these are present. The CSC can appear on the signature strip itself or in a white box to the right hand side of the signature strip. For American Express cards this number has four digits and is printed on the front of the card.

8. Magnetic Stripe

→ Ensure that the card has a magnetic stripe on the back. Be suspicious of a counterfeit if the magnetic stripe feels unusually rough or scratched

→ some cards may have a Holomag tape (holographic magnetic stripe) in place of the traditional magnetic stripe.

9. Ultra Violet Feature

→ If you have an ultraviolet light box for checking banknotes, you can check for the presence of an ultra violet marker on the front of these cards:
  → MasterCard - the letters M and C
  → Visa - dove
  → Maestro - the Maestro logo.

10. Other Features

→ Card logos – these appear on the front of the card and can also appear on the reverse. They should be clearly reproduced with sharp colours – be suspicious of a counterfeit if the logo is ragged around the edges or poorly reproduced

→ Holomag tape – a holographic magnetic stripe. When the holomag is present it must always be on the back of the card, and no other hologram appears on the card

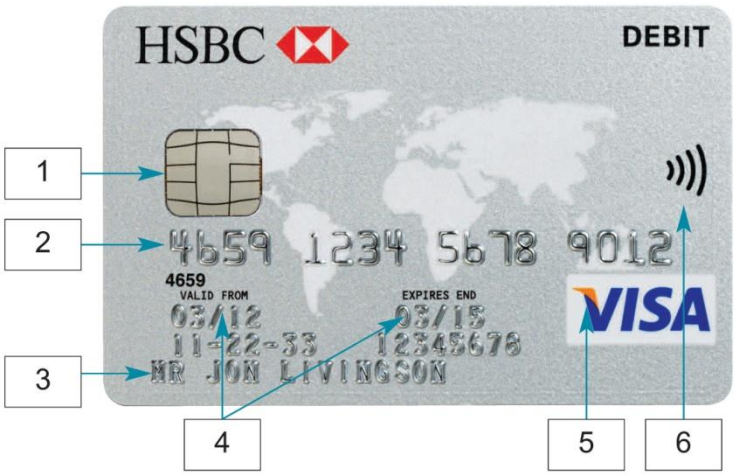
Examples Of Card Types

Key to card images:

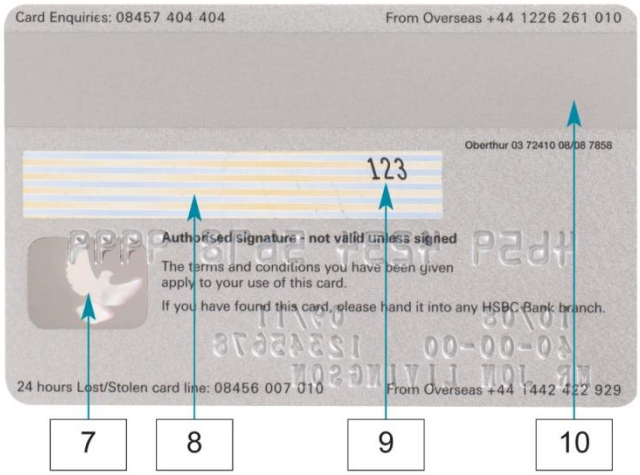
1. Chip
2. Card Number
3. Cardholder Title and Name
4. Valid From/Expiry Date
5. Card Logo
6. Contactless Logo (where present)
7. Hologram
8. Signature Strip
9. Card Security Code
10. Magnetic Stripe

Visa Debit

Front

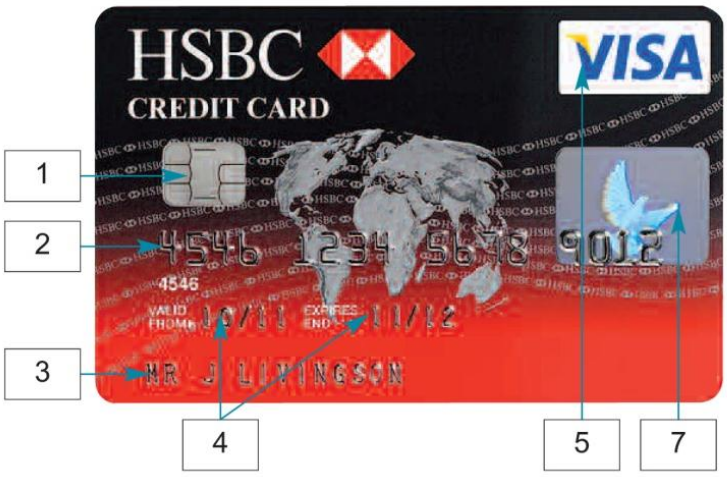


Back



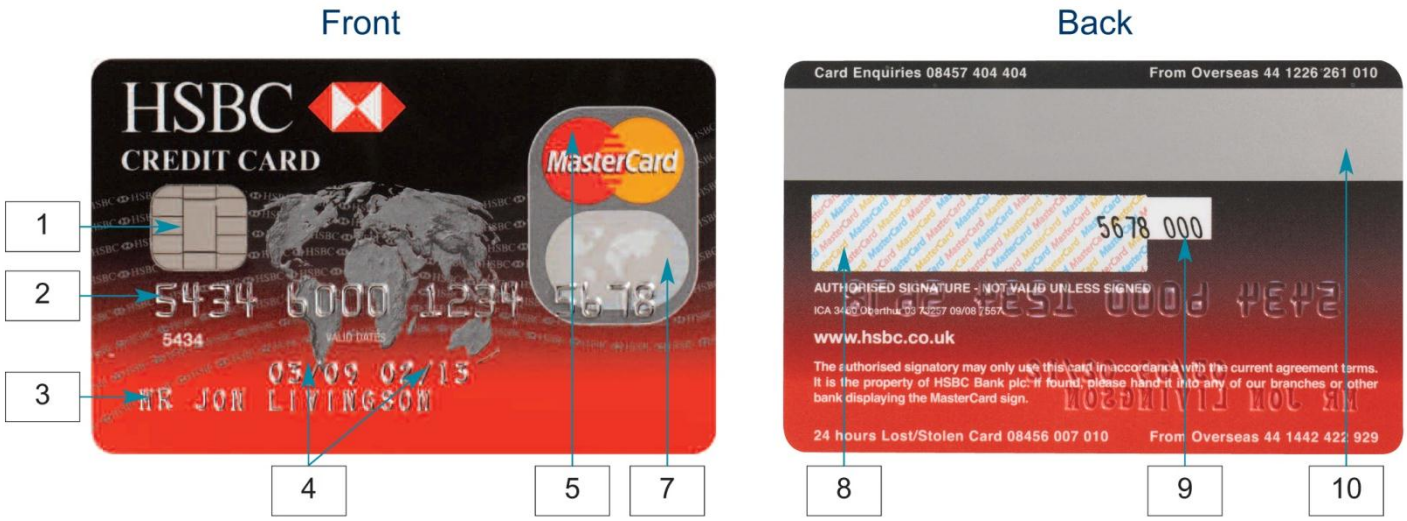
Visa Credit

Front

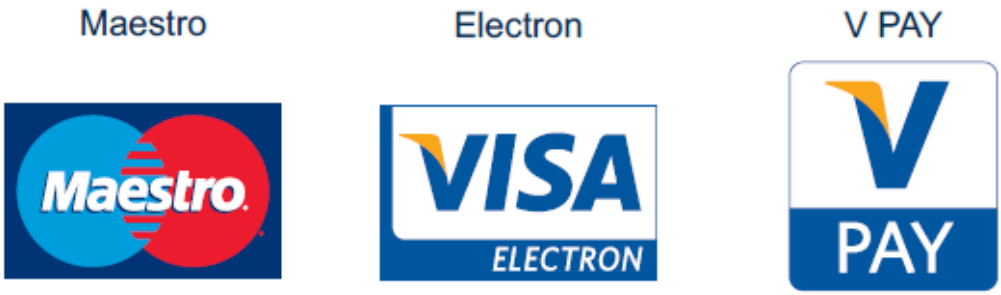


Back

MasterCard Credit



Other Card Logos



Accepting Cards Using An Electronic Card Reader

You can accept cards by using a terminal supplied by Intuit only.

Before you begin:
→ read the terminal user guide before you start using your terminal, as this will provide you with information on the acceptance of cards
→ ensure that any surveillance equipment you have is not able to record a customer entering their PIN

Please visit our support site: www.intuitpay.co.uk/support if you need any help

Authorisation

Authorisation must be obtained at the time of the sale whilst the cardholder is present, in the case of Card Present transactions.

Never spread the value of the sale over more than one card, or split the sale into smaller amounts.

Do not hand over any goods to the cardholder until you have obtained authorisation.

What Is An Online Authorisation?

Online authorisation is when your terminal automatically:
→ checks certain card details
→ seeks confirmation that the cardholder has sufficient available funds on their account at the time of the transaction
→ checks that the card has not been reported lost or stolen at the time of the transaction.
However, it does **not**:
→ confirm the cardholder's identity
→ guarantee payment.

What Message Will Appear On My Terminal?

There are three possible message types for your terminal:

Authorised
This is where the payment has been authorised by the card issuing bank and the transaction has completed. You should now send the customer an electronic receipt either via SMS or email, using the Intuit Pay App.

Not Authorised
You will see this response where the transaction is unable to be completed. This could be due to a communication failure – check your data connection. Alternatively it may be that the card issuer is unable to approve the transaction at the current Time, in which case you should ask for another form of payment.

Transanction Voided
You will see this response on screen where the transaction is cancelled at any point before the transaction has completed, You may wish to show the cardholder your mobile screen so they can see the transaction did not complete.

What To Do When A Card Is Found At Your Premises

Please keep any cards left by customers in a safe place for 24 hours.

When a card is claimed, do not hand over the card until you have verified the cardholder's identity:
→ ask for satisfactory identification, such as a driver's licence
→ check the signature on the card against a specimen signature of the person claiming the card

If the card has not been claimed within 24 hours:
→ Contact the card issuer using the number on the back of the card and advise that the card has been left.

Refunds

→ Refunds can only be made on the card used for the original sale transaction
→ the value of the refund cannot exceed the original transaction amount
→ never make cash or cheque refunds for card transactions.

We recommend that you carry out regular checks to confirm that all refunds made using your terminal/point of sale equipment are genuine. To assist with this, the number and value of refunds made are included in the daily terminal summary report. You may also want to consider restricting the ability to make refunds to certain staff members.

To make a refund undertake the following procedure:
→ **process the refund through the mobile application or your virtual terminal**– see your terminal user guide.

Please note that it is not necessary to obtain authorisation for a refund.

You must state your refund policy clearly to cardholders. Failure to do so increases your vulnerability to chargebacks.

Exchanging Goods

Give a refund for the original sale and complete a new electronic transaction for the full amount of the new goods/services provided.

Cancelling And Reversing Transactions

If a cardholder decides not to purchase the goods or services, you must cancel the transaction. The action you need to take depends on how you have accepted the card and the stage you have reached in the transaction when the cardholder changes their mind.
If you have not completed the transaction:
→ verified by PIN - you can cancel the transaction when you key in the amount. Alternatively the cardholder can cancel the transaction when entering their PIN
→ verified by signature - you can cancel the transaction when the terminal prompts you to confirm the cardholder's signature.

If the cardholder wants to cancel the transaction after it has been completed, perform a refund as outlined on previous page.

How To Submit Your Electronic Terminal Transactions

Online Terminals

These terminals submit transactions to a host system throughout the business day. Overnight the host system will release all stored transactions for processing. Online terminals do not store transactions.

Processing Of Transactions

Providing your transactions have been successfully released by the host system, we will transmit the transactions to the relevant card issuers to request payment from them on the business day after we receive your transactions. If the transactions are not released by the host system until after 6.00am on a business day, or on a day which is not a business day, then your transactions will be treated as having been received on the following business day. For example:

- → if the host systems releases transactions overnight on a Monday, we will transmit them to the card issuers on Tuesday
- → if the host systems releases transactions overnight on a Friday, we will transmit them to the card issuers on Monday (unless this is a public holiday, in which case they will be transmitted on Tuesday).

Card Not Present Transactions

Please note that requirements in this section are provided in addition to those in the remainder of these *Merchant Operating Instructions* and you will need our written agreement to undertake any CNP transactions.

Card Not Present (CNP) transactions are any transaction where the card and cardholder are not physically present with you at the time of the transaction and includes the following types of transaction:

- → mail/telephone/fax transactions conducted by post, fax, telex, telephone or any other similar form of communication
- → internet transactions via computer networks including the internet

These transactions present an opportunity for fraud, as the card, signature and personal identification number (PIN) cannot be checked.

It is vital that you understand the risks associated with CNP transactions. All CNP transactions are accepted at your own risk.

Please read the 'How To Reduce Fraud' section on page 26 which provides important advice on CNP fraud and how to minimise your risk of financial loss.

You must also be compliant with the Payment Card Industry Data Security Standard (PCI DSS) (see 24), a mandatory requirement introduced by the Card Schemes to minimise the possibility of you suffering a security breach.

Please note:

- → **Maestro cards issued outside the UK cannot be used for mail order and telephone order (MOTO) transactions**
- → **Maestro cards cannot be used for recurring transactions.**

Accepting Mail And Telephone Orders

Mail order and telephone orders (MOTO) can be accepted by key-entering the transaction into your virtual terminal through your PC.This is accessed via the Intuit Pay website.

You must ensure that you have the following information from the cardholder:
→ card type
→ Card Security Code (CSC) (see page 11)
→ card number
→ name and initial(s) exactly as they appear on their card
→ valid from date (if on card)
→ expiry date
→ statement name
→ statement address
→ contact telephone number (we recommend that you do not accept a mobile telephone number).

Please note you must destroy any record of the CSC once it has been checked as the retention of the CSC post-authorisation is strictly forbidden under Card Scheme security requirements (see the 'Data Security' section on page 23)

You must inform the cardholder of the total transaction value (including the currency) and obtain their authority to debit this amount from the card.

Never spread the value of the sale over more than one card, or split the sale into smaller amounts.
You must also ensure that:
→ any written orders contain the cardholder's signature
→ you establish a process for checking to see if different transactions relate to the same address, or if the same card number is being used for different addresses
→ for deliveries to the cardholder's address, if possible obtain the telephone number for the delivery address from the directory enquiries service or a local directory, before despatching the goods, telephone the customer back on the number provided to confirm the order.

Confirming Orders

When an order and payment have been accepted, a transaction receipt or confirmation must be provided to the cardholder. This will usually be by e-mail or SMS but if your customer prefers a written receipt, please ensure you include the following pieces of information on the receipt itself:

- Your business name
- City in which your business is located
- Country in which your business is located
- Transaction amount
- Transaction date
- Type of card which you accepted (e.g. Visa Card, Visa Electron, MasterCard, etc.)

Delivering Goods

We recommend that you follow the guidance below. This is particularly important if the goods are of high value.

When delivering goods:
→ Always send goods by recorded or special delivery or by a reputable security carrier. Insist on a signed (preferably by the cardholder) and dated delivery note. Tell the

courier not to make the delivery if the premises appear to be vacant. Please note that proof of delivery alone is not sufficient evidence to defend a chargeback.
- → Do not release goods to third parties such as taxi drivers and messengers.
- → Be cautious of transactions where the billing address is different to the requested delivery address. Avoid delivering to addresses other than the cardholder's, such as hotels, internet cafes and 'care of' addresses.
- → Be wary of requests for next-day delivery, requests to alter the delivery address at short notice, or telephone calls on the day of delivery requesting a specific delivery time.
- →

Collection Of Goods

If the cardholder collects the goods, the transaction will become card present (CP). Ask the cardholder for their card and follow the normal CP procedures. The cardholder must enter their PIN or sign a new terminal receipt. Any previous CNP transaction and associated authorisation must be cancelled, and any record of the CSC and other sensitive card data securely destroyed *(*see page 23 regarding 'Data Security'*)*.

Special Transaction Types

This section will introduce you to a number of special types of transaction that you may need to be familiar with, depending on the way in which you propose to accept card payments.

Please note that requirements in this section are provided in addition to those in the remainder of these *Merchant Operating Instructions* and you will need our written agreement to undertake any of these special transaction types.

Gratuities

A gratuity is an additional amount added to a transaction by the cardholder, for example adding a tip when a cardholder settles a restaurant bill.

See your terminal user guide for further information.

Prepayments/Deposits

This is also sometimes known as a 'delayed delivery' and is typically used for transactions where it is not possible to immediately supply the purchased goods, for example, a large piece of furniture that has to be made to order. In these instances you may require the cardholder to make the purchase as two separate transactions, the first for the deposit and the second for the outstanding balance.

As this poses additional risk to you, you will require written approval from us before you can start to process this type of transaction.

Crediting Your Bank Account

Credits To Your Bank Account

Timescales For Our Processing

Following receipt of your transactions, we will transmit them to the relevant card processors to request payment on your behalf. Amounts received from card issuers in respect of your transactions will be held to your account within our processor, books and records on the same working day (Monday to Friday, excluding public holidays) that they are received. Payment will be made to your bank account, or otherwise, as set out in the *Terms of Service*, for example, into any Reserve Account which is maintained for you. You will generally receive cleared funds in your bank account by the third working day after we receive your transactions for processing. The date the credit appears on your account is dependent on your account holding bank.

Timescales For Your Credit

The following is a guide to when you should expect any payments to be credited to your bank account:

- → if you process cards electronically, and your bank account is held with HSBC Bank, you should be credited with uncleared funds the next working day following successful receipt of your transactions. These funds should clear within the next two working days and will be available for withdrawal the working day **after** they have cleared
- → if you bank elsewhere, you should be credited with cleared funds the third working day following successful receipt of your transactions and will be available for withdrawal the working day **after** they have cleared.

Examples of typical Crediting Timescales are:

- → Monday - transaction undertaken
- → late Monday/early Tuesday - transaction sent to us
- → late Thursday - funds clear
- → Friday - funds are available for withdrawal.

Crediting timescales may vary if:

- → a different crediting delay has been agreed
- → we have agreed any other arrangements in writing
- → you have not followed the *Merchant Operating Instructions*.

Bank Statement Entries

We will credit your nominated bank account with a single credit for all cards, with the description Intuit Pay

Rejected Transactions

As part of our transaction validation process, we will reject and return any transactions that fail validation, for example, an expired card has been used. Rejected transactions will result in financial loss to you.

Before this happens, we will check the transaction details and our systems. If we identify any errors, these will be corrected. If this does not resolve the problem, we will advise you by email and the amount credited to your bank account will be adjusted accordingly.

Service Charges

This is the amount payable by you for our card processing services.
Please refer to the *Terms of Service* for a full explanation of our service charges.

How Will We Collect Service Charges?
Intuit will collect all transaction charges from the daily amount processed and settle to you net of charges.
Other service charges will be collected via Direct Debit in accordance with your invoice.

Reconciliation

We strongly recommend that you reconcile all your bank account entries on a monthly basis. Please email us at: support@intuitpay.co.uk at the earliest opportunity if you have any queries about your card processing statement entries.

Chargebacks

Introduction

A chargeback is a transaction that has been disputed by the cardholder or card issuer and returned to us. A chargeback is also known as a 'dispute'.

Each chargeback has specific rules, regulations and time limits within which Intuit must operate. These are set by MasterCard and Visa and influence the actions we are able to take when dealing with chargebacks. We will do everything possible within the rules to defend the chargeback on your behalf.

There are a number of different reasons why a transaction can be charged back, but they mainly fall into five categories:
- → request for information (see 'What Is A Retrieval Request?' below)
- → fraud – the transaction was completed for an illegal or fraudulent purpose and you were or should have been aware of such illegality or fraud
- → authorisation related –for example, authorisation has been declined etc
- → processing error – for example, duplicate processing of a transaction
- → cancelled/returned goods or service – cardholder has cancelled an order or returned goods and has not received a refund, or a refund has not been processed, or a refund has not been credited to the same cardholder account that was originally debited
- → non-receipt of goods/services - for example, in the case of late delivery of goods or services, or the wrong goods have been delivered.

We will always advise you by email of the chargeback prior to the debit being applied to your account. Whether we can defend the chargeback depends on whether the transaction has complied fully with the rules set by MasterCard or Visa. Where possible, for example, where a transaction has been authenticated by chip and PIN and you are not liable, we will automatically defend the chargeback on your behalf. In the event additional information/documentation is required from you, you will receive notification by email and the disputed amount will be debited to your account.

If we contact you, it is crucial that you return the requested information, in a clear format, to us within the timescale stipulated. Failure to do so may prevent us from taking any further action in defending the chargeback within the time allowed.

Requests for such documentation can be received up to 180 days after the transaction has been debited to the cardholder's account or the service received. However, in some circumstances, for example when fraud is involved, documents can be requested up to

two years after the transaction date. It is therefore essential that you are able to retrieve such documents easily. Remember, card data must be stored securely (see page ? regarding 'Data Security').

Please contact us at: support@intuitpay.co.uk if you need to discuss a chargeback notification or if you are unsure what documentation is required.

What Is A Retrieval Request?

A retrieval request, also known as a request for information, is when a cardholder queries a credit or debit card transaction. This is often because the cardholder cannot remember undertaking the transaction.

A retrieval request is not a chargeback. This means we do not debit any money from your account. However, a retrieval request can turn into a chargeback if the information the card issuer receives from us is illegible or insufficient to satisfy the cardholder's enquiry.

It is important that you reply to a retrieval request immediately because if you fail to do so, under the rules set by MasterCard and Visa, we may lose the right to defend any subsequent chargebacks.

How To Prevent Chargebacks

Card Present (CP) Transactions

Chip and PIN cards and terminals have made substantial advances in preventing card fraud and are now the norm.

Card Schemes require all CP transactions to be performed using a chip and PIN terminal when presented with a chip and PIN card. Fallback from chip to magnetic stripe is allowed if, after inserting the chip, your terminal prompts you to follow this process.

There are still many legitimate cards in circulation that contain no chip and you will have to swipe the magnetic stripe. You may then have to use the cardholder's signature to verify the transaction. Additionally, there are cards that have a chip but ask for the cardholder's signature as verification. Many of these cards have been issued overseas or to cardholders unable to use a PIN.

The best way to minimise the risk of CP chargebacks is to carefully follow the prompts provided by your terminal. If the terminal authorises a payment and prompts the cardholder to sign, then this should be allowed, subject to the normal checks associated with a signature-verified transaction (see page 9).

Card Not Present (CNP) Transactions

In a CNP environment, it is important to remember that you are liable for chargebacks. If you follow the points listed below together with the important information listed in the 'How To Reduce Fraud' section on page 26 your risk will be minimised:

- → if a customer asks to collect the goods, perform the transaction at the time of collection as a cardholder present transaction through your point of sale equipment
- → always send goods by recorded or special delivery or by a reputable security carrier. Insist on a signed (preferably by the cardholder) and dated delivery note. Tell the courier not to make the delivery if the premises appear to be vacant. Please note that proof of delivery alone is not sufficient evidence to defend a chargeback
- → do not release goods to third parties such as taxi drivers and messengers

- → be cautious of transactions where the billing address is different to the requested delivery address. Avoid delivering to addresses other than the cardholder's, such as hotels, internet cafes and 'care of' addresses
- → be wary of requests for next-day delivery, requests to alter the delivery address at short notice, or telephone calls on the day of delivery requesting a specific delivery time
- → be cautious of customers who give mobile phone numbers as their only form of contact
- → be wary of an order emanating from an e-mail account where the customer's name is not reflected in the e-mail account address
- → be suspicious with transactions that have an unusually high value or volume for your type of business or the sale is 'too easy'. In our experience these are the more likely ones to be fraudulent
- → when performing a refund, always refund to the same card used for the original transaction
- → keep a database of chargeback history to help identify patterns of fraudulent transactions. If a sale seems too good to be true then it probably is. Do not be afraid to contact the cardholder to ask further questions or request additional identification. A genuine customer should be pleased you are security minded and trying to protect them from fraud
- → where possible, perform and Card Security Code (CSC) checks (see page 11*).* Refer to your terminal manual or terminal supplier for assistance on using this security feature. May we remind you though that you are **not** allowed to store the CSC data

The majority of chargebacks result from transactions being undertaken fraudulently. If you proceed with a transaction that appears suspicious, then you are doing so at your own risk. If the transaction has been completed, but the goods have not been despatched, you are still in a position to carry out a refund of the transaction.

Obtaining A Successful Authorisation

Please see the 'Authorisation*'* section on page 14 for information on card authorisations.

A credit or debit card authorisation is a way of verifying the card has not been reported lost/stolen and the cardholder has sufficient funds at the time of the call. It does **not,** however, guarantee the transaction.

Deposit Taken - Goods Ordered, But Not Immediately Delivered

This is also sometimes known as a 'delayed delivery' and is typically used for transactions where it is not possible to immediately supply the purchased goods, for example, a large piece of furniture that has to be made to order. In these instances you may require the cardholder to make the purchase as two separate transactions, the first for the deposit and the second for the outstanding balance.

When completing a sale using this method, it is important that the two transactions are processed separately and the second receipt is not processed before the goods have been despatched. If you do process the receipt for the balance earlier than the date that the goods have been despatched, a cardholder may view this as 'goods not received' and request their card issuer to chargeback the transaction.

Under Card Scheme Rules, the transaction receipt for the deposit may be submitted for processing before the delivery of the goods or services. However, the transaction receipt for the balance must not be submitted until after the goods have been despatched. If the difference between the goods being ordered and despatched is less than 30 days, this rule does not apply. In all instances, to help identify the order, the word 'deposit' or 'balance' must also be written on the appropriate transaction receipts.

Non-receipt Of Goods Or Services Not Rendered

- → Do not process a card transaction until the goods have been sent or the services have been provided
- → do not process any credit or debit card transactions where the cardholder has already paid for the goods or services using an alternative method of payment
- → obtain the cardholder's signature on your delivery notes or service sheet following the completion of the service
- → if you are unable to deliver all good or services in full, keep the cardholder informed of your actions at all times

Goods Not As Described

- → You must ensure that the goods ordered by a cardholder are delivered or provided exactly as described in your brochure or advertisement. If you are unable to provide the exact specification including colour, size, quality and quantity, then you **must** notify the cardholder of the change and seek their approval to accept the revised option
- → the goods should be delivered in a timely manner and be suitable for the purpose for which they were ordered, for example theatre tickets that arrive after the date of the performance are not acceptable
- → if goods are received by a cardholder and are damaged, broken or otherwise unsuitable for the purpose for which they are required, then the cardholder will have the right to chargeback the transaction
- → if the cardholder returns the goods to you then you are required to reimburse the cardholder with the total value of the returned goods immediately.

Other Chargeback Reasons

Some other common reasons for chargebacks are listed below. This is not meant to be an exhaustive list and providing you follow the guidelines provided in these *Merchant Operating Instructions*, chargebacks should be avoidable.

- → Late processing – the transaction was submitted late and was processed outside the Card Scheme permitted timeframe
- → transaction processed on an expired card
- → incorrect transaction amount – cardholder charged more than receipt or advice.

Data Security

Security of personal data is a growing concern for everyone and criminals are always looking for ways of obtaining this type of information. Card and financial data are obvious targets for criminals, and as you are accepting card transactions, you need to be aware of the value of the data you collect when undertaking a card transaction and the need to secure it.

If you were to suffer a security breach, there is a significant risk of financial and reputational loss to your business. The major Card Schemes have introduced regulations relating to data security and it is important that you follow them to minimise the risks to your business.

Best Practices

The fundamental principle you must follow is to treat card financial data as you would cash. You should ensure this data is held as securely as possible by:

- → never releasing card information to anyone except us
- → restricting your employees' access to card data.

Do not store the following information under any circumstances:

- → full content of data from the card magnetic stripe or chip - also known as track 2 data

→ the Card Security Code (CSC) (see page 11 - should be deleted as soon as you have authorised the transaction, even in the case of CNP transactions, such as mail order and telephone order (MOTO) or internet transactions.

It is essential that you implement the following procedures:
→ store only the customer's account information that is essential to your business
→ store all material containing card information (e.g. authorisation logs, transaction reports, transaction receipts, customer agreements and carbons) in a locked, secure area
→ destroy or delete all media containing obsolete transaction data with cardholder information
→ advise us of any third parties that engage in, or propose to engage in, the processing or storage of transaction data on your behalf
→ store transaction receipts securely for five years following delivery of goods or completion of the service provided, and then ensure that they are safely destroyed
→ Intuit recommends you do not store cardholder data electronically. If you need to do this the data must be encrypted and you must notify Intuit by email at: support@intuitpay.co.uk

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS and other supporting standards, including but not limited to, Payment Application Data Security Standards (PA-DSS) have been developed by the Payment Card Industry Security Standards Council (PCI SSC) and are implemented by supporting mandates via the Card Schemes. Most major Card Schemes, including MasterCard and Visa, are founder members of this organisation.

Compliance with PCI DSS is mandatory for all merchants and is supported by Card Scheme mandates with compliance programmes for some merchant categories. Typically the current compliance programmes impact all larger merchants (those processing more than 1 million MasterCard or Visa transactions annually) and all merchants who trade in the e-commerce environment, especially the internet, where compliance mandates are in force. There are potentially severe penalties for non-compliance with these mandates. As a card processor, we are contractually obliged to observe Card Scheme Rules and, as a merchant accepting card payments, so are you.

The standards are continually reviewed, and the Card Schemes issue supporting mandates to ensure the standards remain relevant and fit for purpose, particularly in light of fraud trends/activity and consequential losses. Intuit will communicate any changes to these requirements and how they might affect you as and when appropriate.

Further, regularly updated information on all the PCI standards can be found on www.pcisecuritystandards.org.

PCI DSS is a comprehensive standard intended to help you proactively protect customer account data. It covers areas such as:

→ firewalls
→ changing default passwords
→ protecting stored data
→ data encryption
→ anti-virus software
→ information security policy
→ maintaining secure systems
→ unique user IDs for all staff
→ restricting access to data
→ physical security
→ monitoring all system access
→ testing security systems and processes.

If you are developing, reviewing or designing computer systems yourself, or purchasing them via a third party, who store, process or transmit sensitive card data, it is important

that you ensure the system and the third party is PCI DSS compliant.

If you use vendor supplied off-the-shelf software in your point of sale equipment, you are mandated by the Card Schemes to only use valid PA-DSS compliant software. Using non-compliant software breaches Card Scheme Rules and could leave you exposed to significant penalties, with any costs or fines being your responsibility. You are also at an increased risk of a data breach which would have a significant financial impact on your business were it to happen.

For further details on PCI DSS you can visit:
- → www.pcisecuritystandards.org - this site holds the latest version of the PCI DSS specifications and guidance on how to become compliant
- → www.mastercard.com/us/sdp/merchants/index.html
- → www.visaeurope.com/en/businesses__retailers/payment_security.aspx

Third Party Companies

If you are using a third party company and give them access to card and financial data for any purpose (for example, processing transactions, storing data or call centre functions), you will need to ensure that they also adhere to all rules and regulations governing card data security. In particular, all third parties storing or processing this data on your behalf are required to be compliant with the Payment Card Industry Data Security Standard (PCI DSS). Any violations of these requirements by your third party are your responsibility and may result in you having unnecessary financial exposure.

You must only use a third party listed on the Visa Merchant Agent Registration site, http://visamerchantagentslist.com. If any third party you use is not on this list, you must either encourage them to seek a listing – they can do this via https://www.visamerchantagents.com – or you must transfer your business to a third party who is currently on this list. This is to ensure the integrity and security of the payment process through proper regulation of third parties involved in the payment chain and is a Visa Europe mandate. Any non-compliance carries substantial penalties, which we will pass on to you.

If You Suspect A Security Breach

If you have followed the best practices listed above and become fully compliant with PCI DSS, you will have minimised your chances of suffering a security breach. However, security can never be perfect - it is therefore necessary to put an instant response plan in place, tailored to your own business environment, so that you know what steps to take.

If you experience, or even suspect, a security breach at your business which might involve card financial data, it is vital that you take the following precautions:
- → contact us immediately at: support@intuitpay.co.uk
- → do not access or alter compromised systems - do not log on or change any passwords
- → do not turn the compromised systems off; isolate them from your network and unplug any network cables
- → preserve all logs and similar electronic evidence
- → perform a back-up of your systems to preserve their current state; this will facilitate any subsequent investigations
- → log all actions taken.

Additionally, you should obtain professional advice from a PCI DSS approved Qualified Forensic Investigator, details of which can be obtained at:

www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php

How To Reduce Fraud

Financial Fraud Action UK
Working together to prevent fraud

www.financialfraudaction.org.uk

Financial Fraud Action UK raises awareness about all types of plastic card fraud in the UK and provides information to prevent fraudulent use of credit cards, debit cards and charge cards.

In addition, Financial Fraud Action UK provides on-line training for retailers, retail staff and law enforcement agencies and contributes to the fight against plastic card fraud.

The website featured above offers comprehensive information about plastic card fraud, free publications and training materials, as well as useful tips and answers to frequently asked questions.

As an active member of the 'Financial Fraud Action UK' campaign, we ask you to play your part in combating plastic card crime.

Card Present Transactions (CP)

See page 9 for an explanation of CP transactions.

The introduction of chip and PIN has radically changed the face of card fraud within the UK. The success of chip and PIN has led to fraudsters being forced to change their focus to counterfeit fraud outside the UK and card not present (CNP) fraud.

Counterfeit Fraud

The UK has led the world in the introduction of chip and PIN technology. Chip and PIN rollout programmes have now been announced for most of the rest of the world. However, until such time as chip and PIN is universal, there will still be a need to retain the magnetic stripe and signature panel on all cards.

As MasterCard and Visa are global brands, a card issued in the UK is valid in countries that have yet to adopt chip and PIN and, conversely, cards issued in non-chip and PIN countries are equally valid in the UK.

A counterfeit card is a forged card that has been printed, embossed or encoded with the details of a genuine card. Most counterfeit cards are the product of 'skimming', where the data from the card is copied without the genuine cardholder's knowledge. 'Skimming' can occur at retail outlets or cash machines, where the card is put through a device that electronically copies the cardholder data.

Magnetic Stripe Transactions

If you are presented with a magnetic stripe card, undertake the following procedure:

- → check the card (see page 9)
- → does the title on the card that you are given match the person? Check for obvious discrepancies between the cardholder and card, such as a woman using a card with the title 'Mr', or a teenager using a card with the title 'Doctor' or 'Sir'
- → watch out for seemingly random and careless purchases, for example, is the customer buying a large number of the same item?
- → has the customer not bothered to try on the clothes?
- → is the customer nervous or trying to distract you?

- → check the signature and signature strip
- → if signature is legible, does it agree with the embossed name on the front of the card?
- → has the signature strip been tampered with?
- → do the last four numbers printed on the signature strip correspond with the last four digits of the cardholder number on the front of the card?
- → does the embossed card number match the printed receipt? The last four digits of the cardholder number should be printed on the receipt - ensure they match the cardholder number printed on the front of the card.

Card Not Present Transactions (CNP)

See page 16 for an explanation of CNP transactions.

CNP fraud can take place over any channel when the cardholder is not with you in person. It is now the largest type of fraud within the UK and is perpetrated by fraudsters obtaining either the physical card or the details contained within the card. These details can be obtained through a number of methods such as 'skimming', discarded receipts or card statements, 'phishing' for personal data on the internet, and hacking databases containing card and personal information.

Phishing is the name given to the practice of sending e-mails that claim to come from a genuine company operating on the internet. They are sent in an attempt to trick customers into disclosing information at a bogus website operated by fraudsters. These e-mails usually claim that it is necessary to 'update' or 'verify' your customer account information and they urge people to click on a link from the e-mail which takes them to the bogus website. Any information entered on the bogus website will be captured by the criminals for their own fraudulent purposes. For more information please refer to:

www.banksafeonline.org.uk.

There is an inherent risk with CNP transactions because you are unable to guarantee that it is the genuine cardholder providing the information. Therefore, accepting CNP payments considerably increases your vulnerability to fraud, chargebacks and ultimately financial loss. This is because you cannot physically verify the transaction by performing card validation checks and checking the cardholder's signature or PIN.

If you accept CNP transactions, then you will not have the same protection as a customer undertaking face-to-face transactions and you **will** be liable for chargebacks in the future in the event of any dispute.

How Can I Protect My Business?

The fact that a transaction has been authorised does not guarantee payment, it simply means that the card has not been reported lost or stolen or that there are sufficient funds available at the time of authorisation. Authorisation does not authenticate the cardholder.

As there is a greater inherent risk in accepting CNP transactions, it is good practice to conduct further investigations when there are any anomalies with a CNP transaction. These can take the form of standard industry fraud prevention tools and 'common sense' checks to validate a transaction.

Fraud Prevention Tools

The Card Schemes have developed fraud prevention tools such Card Security Code (CSC). Unlike PIN or signature, CSC does not confirm the cardholder's identity, but when used together they offer further information to help you decide whether to proceed with the transaction.

Address Verification Service (AVS):
AVS allows you to confirm that the numeric characters in the billing address provided by the cardholder match the address details held by the card issuer. This check is available for all UK issued cards. A fraudster may be in possession of a card including the CSC, but may not be able to provide the genuine cardholder's address.

Please note that British Forces Postal Office (BFPO) addresses are likely to result in a 'no match' AVS response.

Card Security Code (CSC):
The CSC provides additional security information designed to confirm that the customer is physically in possession of the card. For MasterCard, Visa, and Maestro cards the CSC is the last three digits printed on the reverse of the card after the last four digits of the cardholder account number, if these are present. The CSC can appear on the signature strip itself or in a white box to the right hand side of the signature strip. For American Express cards this number has four digits and is printed on the front of the card.

The CSC can also be referred to as CVV, CVV2 or CVC2.

You must not store CSC data. This is strictly prohibited by the Card Schemes (see page 23 regarding 'Data Security').

Fraud Screening

In addition, if you accept CNP transactions, then we strongly recommend that you introduce fraud screening, to check the validity and history of cards tendered.

As a minimum these checks should include:
→ statement address
→ statement address country
→ number of previous declined transactions on same card or same order
→ delivery address
→ phone numbers
→ same value transactions
→ number of times a card has been used in a given time.

Ten Tips To Help Prevent CNP Fraud

Extra vigilance can help prevent CNP fraud. If sales staff can answer ‘yes’ to one or more of the questions below, it does not mean that the transaction is fraudulent - but it does mean that your staff should consider further checks before proceeding with the transaction.

1. Is the sale too easy? Is the customer disinterested in the price or details of the goods? Are they a new customer? Is the customer’s address in your normal catchment area? If not, why are they ordering from you?
2. Are the goods of a high value or easily re-sold?
3. Is the amount of the sale excessively high in comparison with your usual orders? Is the customer ordering many different items or several units of the same item? Do they seem unlike your usual customer?
4. Is the customer providing details of someone else’s card, for example that of a client or a family member?
5. Is the customer reluctant to give a landline contact phone number? Are they only prepared to give a mobile number?
6. Does the address provided seem suspicious? Has the delivery address been used before with different customer details? Is the delivery or contact address overseas?
7. Is the customer being prompted by a third party whilst on the phone or do they seem hesitant when answering certain questions?
8. Is the customer using more than one card to split the value of the sale?
9. Does the customer seem to lack knowledge of their account?
10. Does the customer seem to have a problem remembering their home address or phone number? Does the customer sound as if they are referring to notes?

E-mail Address

There are two types of e-mail addresses. E-mail access is generally available as part of a customer's subscription to a package from their Internet Service Provider (ISP). Alternatively 'free' e-mail accounts can be used, for example from Yahoo, Hotmail and Google ‘G Mail’.

Many genuine customers utilise ‘free’ e-mail accounts due to the ability to be able to use e-mail wherever there is an internet connection. However, fraudsters favour ‘free’ e-mail accounts due to the anonymity it provides them, and the vast majority of e-commerce fraud is committed where 'free' e-mail accounts have been quoted.

The e-mail address alone should not be used to make a decision as to whether a transaction may be fraudulent. Additional validation should be undertaken if a ‘free’ e-mail address is used.

We recommend that you send the customer an e-mail once an order has been placed. It is highly advisable not to process transactions where the e-mail messenger states it has been unable to deliver the e-mail.

Fraud Screening

In addition to the fraud screening checks recommended in ‘Card Not Present Transactions (CNP)’ within this section, we strongly recommend that you undertake the following additional checks for internet transactions:

→ location of IP (Internet Protocol) addresses in relation to country of card issue/delivery address
→ review frequency of use and whether the addresses are linked to orders from more than one delivery address
→ e-mail addresses, as detailed in the previous section.

Additional Important Information

Keeping You Informed

We will send you regular updates on issues that affect the way in which you accept and process credit and debit card transactions.

It is essential that you read these updates and follow our recommendations, especially regarding mandatory Card Scheme changes. Please contact us at: support@intuitpay.co.uk if you need further help or support or if you are concerned that you are not receiving such information.

Producing Your Own Advertising

If you want to produce your own materials to tell your customers that you accept cards as a means of payment, please refer to the MasterCard and Visa websites for copies of the relevant card scheme logo's.

. Please note that the following rules apply:

- → the card logos have been registered as trademarks and must be used in accordance with the instructions contained in the artwork pack
- → the card logos must not be featured in advertising in a way that suggests that the Card Schemes are endorsing your goods or services
- → you must submit all promotional or sales material that refers to us, or any card type, for our approval

Each of your outlets and their points of sale must be clearly identified in the appropriate promotional material.

How To End The Card Processing Agreement

We have every confidence that you will be satisfied with our service. However, if you want to end the Agreement for any reason (other than breach of the Agreement by us) please contact us at: support@intuitpay.co.uk

Full details on how to end the Agreement are set out in our *Terms of Service*.

How To Contact Us

Please reference your merchant number when you contact us. We assign you a merchant number to help us identify you. It appears on your monthly invoice and on receipts from your electronic terminals.

We can be contacted via email to: support@intuitpay.co.uk

Or write to us at:

Intuit Pay
Statesman House
Stafferton Way
Maidenhead
SL6 1AD

If You Want To Complain

If for any reason you are not entirely satisfied with any aspect of our service, we want to hear from you as soon as possible. We will then make the relevant enquiries and aim to put matters right as soon as we can.

Please begin by emailing our support team at: support@intuitpay.co.uk and telling us where the problem has arisen. We will try to answer your concerns straight away, and if we cannot do so there and then, we will investigate and get back to you back as soon as we can.

If you subsequently feel we have not resolved the problem to your satisfaction, you can escalate your complaint to our regulated partner, HSBC Merchant Services LLP, via their head office at:

Customer Relations Department
HSBC Merchant Services LLP
51 De Montfort Street
Leicester
LE1 7BB

They will send you written acknowledgment of your complaint within five working days of receiving your letter. This will confirm that they have received and recorded your complaint.

We always want to be able to resolve any concerns you raise with us. However, where you are not satisfied with the response, or if you have not received a reply from HSBC Merchant Services LLP within eight weeks, you may have the right to refer the complaint against HSBC Merchant Services LLP to the Financial Ombudsman Service.

The Financial Ombudsman Service

The Financial Ombudsman Service deals with some types of complaints from private individuals, together with businesses and charities with an annual turnover of less than two million euros **and** has fewer than ten employees.

Call: 0800 023 4567 – calls to this number are free when calling from a fixed line in the UK, or
0300 123 9123 – calls to this number are charged at the same rate as 01 or 02 numbers on mobile phone tariffs

Please note calls to both these numbers are recorded.

E-mail: complaint.info@financial-ombudsman.org.uk

Write to: The Financial Ombudsman Service
South Quay Plaza
183 Marsh Wall
London
E14 9SR

Or visit at: www.financial-ombudsman.org

Intuit Pay is a trading name of Intuit Ltd, who are an approved agent of HSBC Merchant Services LLP. HSBC Merchant Services LLP is authorised by the Financial Services Authority under the Payment Services Regulations 2009 (504290) for the provision of payment services.